Random neural network based intelligent intrusion detection for wireless sensor networks

Saeed, Ahmed; Ahmadinia, Ali; Javed, Abbas; Larijani, Hadi

Published in:
Procedia Computer Science

DOI:
10.1016/j.procs.2016.05.453

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Procedia Computer Science

Volume 80, 2016, Pages 2372–2376

ICCS 2016. The International Conference on Computational Science

Random Neural Network based Intelligent Intrusion Detection for Wireless Sensor Networks

Ahmed Saeed[1], Ali Ahmadinia[2]*, Abbas Javed[1], and Hadi Larijani[1]

[1] Glasgow Caledonian University, Glasgow, UK
[2] California State University San Marcos, San Marcos, California, USA
aahmadinia@csusm.edu

Abstract

Security and privacy of data are one of the prime concerns in today's embedded devices. Primitive security techniques like signature-based detection of malware and regular update of signature database are not feasible solutions as they cannot secure such systems, having limited resources, effectively. Furthermore, energy efficient wireless sensor modes running on batteries cannot afford the implementation of cryptography algorithms as such techniques have significant impact on the system power consumption. Therefore, in order to operate wireless embedded devices in a secure manner, the system must be able to detect and prevent any kind of intrusions before the network (i.e. sensor nodes and base station) is destabilized by the attackers. In this paper, we have presented an intrusion detection mechanism by implementing an intelligent security architecture using Random Neural Networks (RNN). To validate the feasibility of the proposed security solution, it is implemented for an existing wireless sensor network system and its functionality is practically demonstrated by successfully detecting the presence of any suspicious sensor node and anomalous activity in the base station with high accuracy and minimal performance overhead.

Keywords: Intrusion detection, low-power embedded devices, illegal accesses, random neural networks

1 Introduction

The availability of low-cost typical components has changed the world of embedded systems and it has enabled designers to connect devices, including but not limited to industrial sensors, smart phones, medical devices, household appliances, cars and other vehicles to the Internet. There are two key characteristics that make such systems prone to the security attacks. Firstly, the simplified processing capabilities and limited power resources expose them to a number of possible security attacks. Secondly, the network connectivity to the outside world, without any inbuilt protection, also leaves such systems vulnerable to security attacks. In a typical embedded

*Corresponding Author

 Selection and peer-review under responsibility of the Scientific Programme Committee of ICCS 2016

doi:10.1016/j.procs.2016.05.453

system, these vulnerabilities can be exploited by an attacker to steal private data, drain the power supply, destroy the system, or modify the system behavior for other than its designed purpose. Furthermore, advancements in communication technology has also resulted in direct communication for example in smart electric meters, remote controlled devices and wireless sensor nodes. As system components are interconnected and also accessible via Internet, they are at increased risk of security attacks. Therefore, security-awareness is becoming a primary design objective.

Most of existing sensor nodes are micro-controller based embedded devices relying on batteries where reducing energy consumption is a top priority. Normally such devices have zero security due to limited resources and therefore cannot afford security solutions like anti-virus and cryptography [7]. In such embedded devices, the information transmitted by the nodes can be interfered and the application running on the micro-controller can also be compromised. In this way, at least the application data will be corrupted which results in its incorrect execution. We will demonstrate in our case study that without proper security mechanism, the wireless sensor nodes can be manipulated and the base station can be compromised easily if the attacker is familiar with the communication protocol and hardware architecture.

In this paper, a fast and effective anomaly based intrusion detection mechanism (IDM) is presented to detect a wide range of data integrity and performance degradation attacks in the low-power wireless sensor network systems. It is based on learning normal behavior of the system using RNN taking diverse dataset, covering both valid and invalid cases, as input parameters. The trained RNN model is then embedded in the base station of the system to detect any anomalous behavior and prevent its propagation. The proposed solution effectiveness and performance overhead is measured for an existing system consisting of sensor nodes transmitting data to a base station. Through experimental setup it is shown that without proper security mechanism it is possible to intrude into the application running on the base station. Furthermore, it is also demonstrated that the base station successfully detected the presence of the malicious sensor node when the given system is enabled with the proposed IDM.

2 Related Work

Intrusion detection has been studied widely in the perspective of computer networks as they have been the prime target of security attacks. It is also becoming one of the key research areas in the field of embedded systems due to their increasing functionality and connectivity. Different solutions have been proposed to detect and prevent security attacks either through dedicated hardware modules or software-based mechanisms. Currently, various security techniques have been presented in the literature such as reference monitors, cryptography and neural network based intrusion detection solutions.

Most of the reference monitor related solutions are based on scanning processor-executed code by comparing it to a predefined model and the security subsystem operates in parallel with each processor [4]. The hardware-assisted security monitors [5, 9] are based on the concept of sensing deviation in program execution at run-time by comparing behavior against a static model for the purpose of detecting code modification attacks. Mao and Wolf [5] have used hash-based patterns for basic blocks comprising of fewer instructions. Similarly, Yoon et al. [9] presented a security solution for multi-core systems that is based on running monitoring program on a dedicated core.

Security attacks that target confidentiality and integrity of the data can be avoided by encrypting the data. However, such techniques are not realistic for low-power embedded devices due to resource constraints and large power consumption overheads.

Different anomaly based intrusion detection techniques have been proposed in the literature based on machine-learning techniques by learning a model, depicting both normal and anomalous behavior of the system. Viera et al. [8] have used ANN in the cloud environment for anomaly based intrusion detection. They have used a large feature vector for training the model and presented that the ANN can be used to detect intrusions more effectively. The detection accuracy of ANN based models is dependent on the input feature vector and number of hidden layers used in the training phase. Furthermore, the detection phase of such intrusion detection systems is computationally intensive and requires more time to detect any anomaly. Gelenbe [1] proposed the new class of ANN as RNN which is based on concepts of probability theory applied to Markovian queuing theory. RNN is easy to implement on hardware as its neurons can be represented by simple counters [6]. Mohamed and Rubino [6] compared RNN with ANN and showed that training time for RNN is greater than ANN, but RNN outperformed ANN during run-time phase in total calculation time. They further showed that RNNs have strong generalization capability for the patterns not covered in the training phase.

The existing neural networks based intrusion detection solutions are computationally intensive, rely on extensive profiling of the communication traffic and have been designed for systems with ample resources where power consumption is not a design constraint. Therefore, such solution cannot be deployed for battery operated wireless sensor systems. On the other hand, our proposed solution is based on a RNN model which is easy to implement, has low memory footprint, consumes minimal power and can detect any deviation in the system behavior effectively.

3 System Architecture

Detecting abnormality based on behavior analysis involves learning of the normal operation of the system and identification of any event that deviates from the previously learned model. In this way, unknown security attacks can also be detected which normally left undetected by the signature-based techniques. The proposed intrusion detection mechanism (IDM) uses the Random Neural Network (RNN) to detect any abnormality in the behavior of the system. A previously designed smart controller [3], as shown in Figure 1, has been used to implement the proposed IDM. The system comprises of a base station, sensor nodes and a web server.

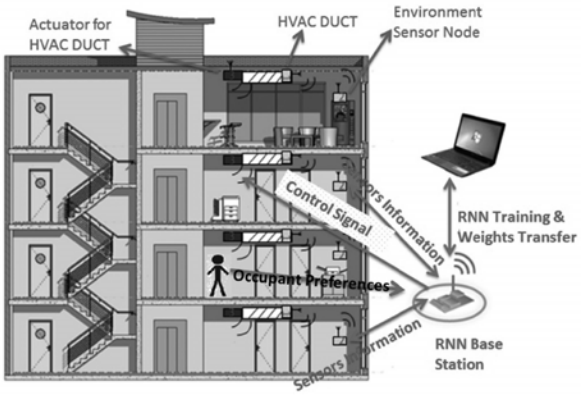

Figure 1: Smart Controller Wireless Sensor Network

This has been designed using multiple RNN models, which have been implemented on low

cost Arduino boards. The base station is developed on an Arduino Mega board and it is connected with control panel of the environment chamber to turn on/off heater, cooler, and ventilation. Each sensor node transmits the data to base station in the form of a string with the following format [node ID, CO2, temperature, humidity, light, and intensity (optional)]. This smart controller is capable of detecting and estimating the number of occupants inside the building in order to turn on/off the Heating, Ventilation and Air Conditioning (HVAC) control. In addition, it can interact with occupants to maintain the occupant preferred set points for heating and cooling. The application running on the base station processes data after receiving it from the sensor nodes through a transceiver and further communicates with a web server through a on-board WiFi module. The sensor nodes are battery operated and cannot afford to send data in encrypted form as it consume considerable amount of power.

4 Evaluation and Experimental Results

The effectiveness and overheads are evaluated by implementing the proposed IDM within the application running on the base station. In the first step, a malicious node is introduced into the system which compromises the base station and in the second step, it is shown that our solution can successfully detect and prevent such attacks with minimum impact on the system resources, performance and power consumption.

The proposed IDM is mainly responsible to detect performance degradation attacks such as detection of invalid packets transmitted by a malicious sensor node with the aim to drain battery and unnecessary utilization of system resources (i.e base station transceiver). Any data corruption as the result of buffer overflow will also be detected by the proposed IDM as long as the application's data memory is intact and program instructions are executing. As the sensor nodes are battery operated, the encryption support has been disabled to save the power. The effectiveness of the proposed solution has been tested under different attack scenarios. To practically evaluate these attack scenarios, we placed a malicious sensor node in the range of base station. This malicious sensor node can transmit the packet containing more data as intended to receive or even transmitting packets containing invalid data. The length and format of data transmitted by valid sensor nodes is analyzed by placing another receiving node. Then the attacker sensor node starts transmitting its own packet leading to performance degradation and generating buffer overflow in the memory where the received data is being stored by the base station. In this way, the base station fails to execute the code in the correct manner. On the contrary, when the base station is protected with our proposed IDM, the security attacks are detected successfully and an alarm signal is generated for further action.

Table 1: Overhead of the proposed Intrusion detection and prevention mechanism

Security Level	System Execution Time (ms)	Power Consumption (mW)	Data Transfer Rate ($kbps$)	Dedicated Hardware Logic	Packet Length$^{\beta}$ ($bytes$)
Baseline	8.584	72	31.69	–	255
AES Encrypted	8.623	86.90	31.54	YES	64
Change*	+0.45%	+20.69%	-0.54%		
Proposed IDM	8.794	78.545	30.93	NO	255
Change*	+2.45%	+9.09%	-2.40%		

[1]*Percentage change with respect to baseline,
$^{\beta}$Maximum length of a packet that can be received/transmitted in a single event

Beside verifying the effectiveness of the proposed IDM, its impact on the system performance, power consumption, data transfer rate and hardware resources has been analyzed. Initially these values have been measured for the baseline application running on the base station without encryption and IDM. Then these values are measured with encryption enabled and finally for the proposed IDM. As shown in Table 1, the proposed IDM has minimal impact on the system. The transceiver module on the base station has hardware 128-bit AES encryption support whereas our IDM does not require any dedicated hardware. Although, the encryption enabled base station has lower execution time but it has higher power consumption compared to our proposed IDM. The encrypted communication also have a significant impact on the sensor nodes power consumption as each node has to transmit encrypted data, consuming more power for each sensor node in the system. Moreover, this encryption is only supported to transmit/receive packets with maximum data length of 64 bytes [2]. Therefore, to transfer large packets, the power consumption of the encryption enabled base station will increase. On the contrary, our proposed IDM has no such restriction as it is not dependent on the packet data length.

5 Conclusion

In this work, we have presented an effective intrusion detection mechanism for low-power wireless sensor networks. An intelligent anomaly detection model is learned using RNN to deal with performance degradation attacks. The feasibility of the proposed solution is demonstrated for a wireless sensor nodes based system, with the detection accuracy of 97.23%. The effectiveness of the proposed solution is further tested by adding attacker sensor node and generating different security attacks that are eventually detected by our solution. The proposed IDM does not require dedicated hardware resources and presented negligible performance overhead with 10.45% increase in the power consumption.

References

[1] Erol Gelenbe. Random neural networks with negative and positive signals and product form solution. *Neural computation*, 1(4):502–510, 1989.

[2] HOPERF. RFM69 ISM TRANSCEIVER MODULE. http://www.hoperf.cn/upload/rf/RFM69-V1.3.pdf, last viewed January 2016.

[3] A. Javed, H. Larijani, A. Ahmadinia, R. Emmanuel, D. Gibson, and C. Clark. Experimental testing of a random neural network smart controller using a single zone test chamber. *Networks, IET*, 4(6):350–358, 2015.

[4] Georgios Kornaros and Dionisios Pnevmatikatos. A survey and taxonomy of on-chip monitoring of multicore systems-on-chip. *ACM Trans. Des. Autom. Electron. Syst.*, 18(2):17:1–17:38, April 2013.

[5] Shufu Mao and T. Wolf. Hardware support for secure processing in embedded systems. *Computers, IEEE Transactions on*, 59(6):847–854, 2010.

[6] S. Mohamed and G. Rubino. A study of real-time packet video quality using random neural networks. *Circuits and Systems for Video Technology, IEEE Tran. on*, 12(12):1071–1083, 2002.

[7] W. Trappe, R. Howard, and R.S. Moore. Low-energy security: Limits and opportunities in the internet of things. *Security Privacy, IEEE*, 13(1):14–21, Jan 2015.

[8] Kleber Vieira, Alexandre Schulter, Carlos Westphall, and Carla Westphall. Intrusion detection for grid and cloud computing. *IT Professional*, 12(4):38–43, 2010.

[9] Man-Ki Yoon, S. Mohan, Jaesik Choi, Jung-Eun Kim, and Lui Sha. Securecore: A multicore-based intrusion detection architecture for real-time embedded systems. In *Real-Time and Embedded Technology and Applications Symposium (RTAS), 2013 IEEE 19th*, pages 21–32, April 2013.